



## Integrated Solutions for Regulatory Compliance With Windows Server Technologies

Microsoft Corporation

Published: October 2004

*The descriptions of certain U.S. laws and regulations in this white paper are provided for general information purposes only, and are not intended to be, nor should be construed as, legal advice from Microsoft. You should always seek the advice of your own legal counsel with respect to any particular issue.*

---

### Abstract

Creating a solution to meet regulatory compliance is a complex process. This solution blueprint helps organizations implement for 3,000 or fewer information workers a data lifecycle solution that uses Microsoft Exchange Server 2003, Microsoft SharePoint™ Portal Server 2003, Microsoft Windows® Storage Server 2003, KVS Discovery Accelerator, and KVS Enterprise Vault. KVS Enterprise Vault provides a powerful platform for data archiving, and KVS Discovery Accelerator enables searching and retrieval of the data within the Enterprise Vault. With this solution, there is no need to restore backup tapes for discovery purposes. All data is readily available to be quickly and efficiently retrieved. The instructions in this solution blueprint enable the reader to integrate KVS Discovery Accelerator and KVS Enterprise Vault into an existing Exchange Server 2003 organization.



Microsoft  
**Exchange Server 2003**

*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.*

*Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.*

*© 2004 Microsoft Corporation. All rights reserved.*

*Microsoft, Active Directory, Outlook, SharePoint, SQL Server, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

---

## Contents

<b>Introduction.....</b>	<b>1</b>
Current Business Environment .....	1
Solution Components.....	2
Exchange Server 2003.....	2
KVS Enterprise Vault and Discovery Accelerator .....	2
Windows Storage Server 2003.....	3
Using This Solution Blueprint.....	3
<b>The Importance of Data.....</b>	<b>4</b>
Creating Data Retention Policies .....	4
<b>Current Regulatory Environment.....</b>	<b>6</b>
Sarbanes-Oxley Act.....	6
SEC Rule 17A-4.....	6
Gramm-Leach-Bliley Act .....	6
Healthcare Insurance Portability and Accountability Act of 1996 .....	6
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).....	7
Department of Defense Rule 5015.2-STD .....	7
National Archives and Records Administration.....	7
CFR Title 47, Part 42—Telecommunications .....	7
CFR Title 21, Part 11—Pharmaceuticals .....	7
<b>Retaining Messaging Data.....</b>	<b>8</b>
Data Archiving and Retention .....	8
What Data?.....	8
How Long? .....	9
Who Can Access the Data? .....	9
Who Should Manage the Data? .....	9
Where Should the Data Be Stored? .....	10
Data Retention Benefits .....	10
<b>Message Journaling Considerations.....</b>	<b>12</b>
Standard Message Journaling .....	12

Exchange Server Envelope Journaling Capabilities .....	12
Message Journaling and Performance .....	13
Exchange Server 2003 Message Journaling Planning .....	14
Analyzing Data .....	15
KVS Enterprise Vault Integration and Features .....	16
KVS Enterprise Vault Discovery Accelerator Integration and Features .....	17
<b>Implementing the Solution .....</b>	<b>19</b>
Solution Component Architecture .....	19
KVS Discovery Accelerator .....	20
KVS Enterprise Vault .....	20
Exchange Server 2003 .....	21
SharePoint Portal Server 2003 .....	21
SQL Server 2000 .....	21
Windows Storage Server 2003 .....	21
Creating Your Own Solution .....	22
Introduction .....	22
Installation Summary .....	22
Configuring Windows Server 2003 for Enterprise Vault, Part 1 .....	22
Configuring Windows Server 2003 Domain Controller .....	24
Configuring Exchange Server, Part 1 .....	25
Configuring Windows Storage Server 2003 .....	26
Configuring Windows Server 2003 for Enterprise Vault, Part 2 .....	27
Configuring Exchange Server, Part 2 .....	33
Configuring SQL Server 2000 .....	33
Configuring Windows 2003 Server for Discovery Accelerator .....	34
<b>Discovery Accelerator in Action .....</b>	<b>36</b>
<b>Installing and Configuring Optional Solution Components .....</b>	<b>44</b>
Enabling SharePoint Portal Server 2003 Archiving .....	44
Supplemental Installation for End-User Archive Access .....	44
Adding an Archiving Service for Users .....	44
Requirements for Users' Computers .....	45

<b>Conclusion .....</b>	<b>46</b>
<b>Related Links .....</b>	<b>47</b>

---

## Introduction

Microsoft® Exchange Server 2003—the best selling messaging and collaboration server—combined with storage solutions powered by Microsoft Windows® Storage Server 2003 and intelligent archiving solutions from KVS, Inc. (KVS), enables organizations to preserve e-mail correspondence as a business record that can withstand scrutiny in court or during regulatory review. Together these products offer document lifecycle management—the ability to capture, archive, and destroy data based on corporate policies, with an audit trail that ensures compliance. For organizations that need to implement an efficient, cost-effective approach for meeting document lifecycle management, Microsoft and KVS deliver a robust set of familiar, adaptable, and dependable tools that make the most of existing information technology (IT) investments to meet immediate and evolving requirements.

Microsoft and KVS together present this solution blueprint to help organizations comply with regulatory requirements. The deployment guidance in this document is:

- **Proven:** This deployment guide is based on practical experience.
- **Authoritative:** This guide represents the best advice available.
- **Accurate:** The information in this guide is technically validated and tested.
- **Actionable:** The procedures and advice are directly usable in projects.
- **Relevant:** This guide addresses real-world scenarios.

Microsoft Windows Storage Server 2003, Exchange Server 2003, Microsoft Office SharePoint Portal Server 2003, KVS Enterprise Vault, and KVS Discovery Accelerator integrate to create this prescriptive framework for message and document archiving.

## Current Business Environment

Over the past decade, e-mail has become critical to many businesses. For many companies, however, management of e-mail as a business record has not kept pace with its importance. Today many companies archive and retrieve e-mail on an ad hoc basis. Few have clearly defined policies about using messaging, what sorts of data is to be transmitted, and what types of protection their messaging data must have. Many organizations are only now realizing that they need a system to ensure that data within their Exchange Server messaging systems is safely stored in a searchable, retrievable format.

Although not all business messaging regulations require message archiving, the regulatory environment is changing, and all businesses should be aware of how changes might affect messaging systems operations in the long term. Some businesses—those in the financial and healthcare industries, for example—have long been aware of the need to archive and track their communications because of such regulations as SEC Rule 17A-4 and Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA). Now, however, industries that have not previously felt the need to retain e-mail data may face these requirements. Regulations such as the Sarbanes-Oxley Act of 2002 (SOX) have highlighted the need for all industries to maintain, store, and secure data, including electronic messages, for several years.

In conjunction with Exchange Server, Enterprise Vault provides the ability to archive, or journal, messaging data sent within an organization and to and from external systems, and it enables organizations to search and retrieve archived data quickly. This capability is vital to ensure that an organization's communications are captured and verifiable.

## **Solution Components**

The major solution components include Exchange Server 2003, KVS Enterprise Vault and Discovery Accelerator, and Windows Storage Server 2003. This section briefly describes these components.

### **Exchange Server 2003**

Message journaling within Exchange Server gives organizations the ability to archive messages sent between their users and external Internet addresses. With minor configuration changes, all internal messages can also be archived. Service Pack 1 for Exchange Server 2003 introduces enhanced journaling capabilities that enable KVS to provide a richer archiving toolset.

### **KVS Enterprise Vault and Discovery Accelerator**

KVS delivers document and e-mail archiving solutions using Enterprise Vault 5 with Cumulative Patches (CP) 1 for Exchange Server and SharePoint Portal Server implementations.

Enterprise Vault 5 CP1 offers a single interface for archived e-mail, SharePoint file system documents, and instant messages. The content archiving solution of Enterprise Vault along with the Discovery Accelerator add-on does the following:

- Reduces the ongoing cost of e-mail storage
- Brings control to mailbox management
- Optimizes backup and recovery cycles
- Ensures that valuable information can be retrieved quickly and efficiently for regulatory compliance and knowledge management

KVS Compliance Accelerator for Enterprise Vault can also provide additional capabilities to meet requirements for lifecycle management and to alleviate business risk. Enterprise Vault enables you to do the following:

- Consolidate Exchange servers
- Eliminate .pst files from your environment
- Archive data in file servers
- Migrate data in public folders
- Archive current data in mailboxes
- Meet regulatory compliance goals

All messages in the Enterprise Vault archive are stored in both their original .msg format and in either plain text or HTML format. The message archive also supports envelope journaling, which retains all pertinent message-related data.

Users can browse the archive and view messages by using Microsoft Internet Explorer from any workstation if they have the correct access permissions. Enterprise Vault also provides client access through Microsoft Office Outlook® and Outlook Web Access for users both online and offline. These capabilities do not hinder information workers from using Microsoft technologies as they normally do.

The integration of Enterprise Vault with your SharePoint Portal Server implementation enables documents to be archived for future reference and recovery. The aggregation of enterprise content enables information workers to better communicate and collaborate and ensures that content will be deleted at the end of its legal and useful life.

KVS Discovery Accelerator provides a fully managed review process that enables roles to be assigned to users within the organization. It offers reviewers a flexible marking scheme so that data can quickly be marked as pertinent. The powerful search capability of Discovery Accelerator makes finding content simple, and items can be produced quickly for disclosure to external reviewers.

### **Windows Storage Server 2003**

In the solution described in this blueprint, Windows Storage Server 2003 hosts KVS Enterprise Vault archives. Windows Storage Server provides dependability, seamless integration, and the best value in networked storage. Windows Storage Server is ideal for organizations that want to consolidate such data as Enterprise Vault archives into a single solution that reduces cost and provides policy-based management of storage resources.

Windows Storage Server includes advanced availability features such as point-in-time data copies, replication, and server clustering. Because Windows Storage Server solutions are preconfigured, they can be deployed in minutes and require little expertise to set up. The Web-based user interface makes management easy. Preconfigured Windows Storage Server solutions ranging from a few hundred gigabytes to several terabytes are available from OEMs such as Dell, EMC, Fujitsu, HP, and NEC.

### **Using This Solution Blueprint**

This blueprint discusses how to use message archival systems, as well as which protection strategies and solutions are best for ensuring that data is properly stored and maintained. In particular, this solution blueprint:

- Provides information about messaging data retention
- Clarifies how Microsoft and KVS can enable businesses to move in the right direction today
- Helps you implement a solution that meets your organization's needs for data retention

As you read this blueprint and begin to plan your own solution, keep in mind that you do not have to build a solution from the ground up because Exchange Server has basic journaling and archiving capabilities, and KVS provides out-of-the-box solutions that enhance the message journaling and retrieval capabilities of Exchange Server.

Unless otherwise noted, this solution blueprint assumes that your organization uses Microsoft Windows Server™ 2003 operating system with Active Directory® directory service and Exchange Server 2003.



---

## The Importance of Data

Today's information workers use their Exchange servers all day, every day. Office Outlook 2003 is the first application that most end users open upon arriving at the office, and it's the last thing they check before going home at night. More and more often, users check and respond to e-mail outside of business hours by using Outlook Web Access, RPC over HTTP, or over a VPN connection. Exchange Server has become a critical application in the quest for productive, efficient businesses. Today contracts are negotiated over e-mail, and documents are attached to messages for review; paper memos are becoming obsolete as they are replaced by electronic communications. Using the vast amount and kinds of electronically stored communication data requires efficient searching methods.

The number of communication and messaging options (and the heightened emphasis on tracking and auditing business records and correspondence) means that it is vital for businesses to be able to track and find data relating to their internal operations and to both their internal and external interactions and communications. The challenge is finding and implementing a system that efficiently manages this data, stores the data in its original format, and allows the data to be discovered.

Exchange Server 2003, the latest version of the Exchange Server messaging and e-mail-based collaboration server, is specifically designed to address business requirements for heightened security in today's computing environments. In accordance with the Microsoft companywide Trustworthy Computing Initiative, Exchange Server 2003 running on Windows Server 2003 provides many new features and enhancements to improve reliability, manageability, and security.

SharePoint Portal Server provides an enterprise portal and document management system by allowing users to store, access, and search for information. Properly managing this data is imperative: Corporate knowledge is an invaluable asset that must be adequately protected and retained, not only for compliance purposes but also to retain the business value of past efforts.

The ability of SharePoint to manage the entire document chain—authoring, versioning, and publishing—lets businesses easily implement an out-of-the-box solution for workflow processes. The integration of KVS Enterprise Vault with SharePoint Portal Server enables organizations to manage the lifecycle of documents based on the business's retention policy and regulatory requirements.

With the inherent flexibility of SharePoint Portal Server, businesses can create separate sites for compliance-related documents and official communications, such as memoranda. The data in these sites may then be archived by using KVS Enterprise Vault and searched and retrieved by using KVS Discovery Accelerator.

## Creating Data Retention Policies

Creating data retention policies involves two entities: stakeholders and deliverables.

Business stakeholders should participate in representing the primary organizations of the company, including representatives from the legal, financial, and IT departments. Involving the appropriate stakeholders helps ensure that policies are not only legally correct but also adequately protect your organization's interests and can realistically be implemented and enforced. This group should consider the risks and realities of your organization's structure and define policy implementation precisely.

This stakeholder team is tasked with recommending ways that the business will meet compliance-related regulations. In particular, the team should:

- Determine what data should be considered official business communication or records
- Develop a comprehensive written policy for data retention
- Educate information workers on how to follow these policies

If your organization does not already have a comprehensive electronic messaging policy, the stakeholders should develop one along with its data retention policies. A comprehensive electronic messaging policy does the following:

- It defines acceptable use of the system, including:
  - Whether system users may send and receive personal e-mail
  - Whether e-mail solicitations are allowed
  - That harassing or threatening e-mail messages are not allowed
  - That transmitting potentially offensive images using the messaging system is prohibited
- It states that users cannot send company-confidential data to third parties except for legitimate reasons.
- It warns that illegal use of the system will not be tolerated.
- It clearly defines retention periods for communications—particularly for businesses that are subject to specific regulations defining retention periods.

When creating an electronic messaging policy, ensure that the correct stakeholders from your organization are involved and that the policy is not created in a vacuum. Your legal department, financial advisors, and system managers must coordinate their efforts in order to create a policy that is not only legally correct, but also adequately protects the interests of your organization, and can be implemented and enforced. The risks and realities of your organization's structure must be considered, and the implementation of the policy should be clearly structured.

The SANS (SysAdmin, Audit, Network, Security) Institute, a cooperative research and education organization, provides a sample policy for e-mail retention at [http://www.sans.org/resources/policies/e-mail\\_retention.pdf](http://www.sans.org/resources/policies/e-mail_retention.pdf). This sample policy may help you create a policy for your organization.

---

## Current Regulatory Environment

The numerous federal regulations relating to records affect organizations of all kinds. Although the financial industry has long been overseen by the Securities and Exchange Commission (SEC) and National Association of Securities Dealers (NASD) and the healthcare industry has rushed to meet the requirements of HIPAA, other types of organizations must now respond to federal regulations. Since the enactment of more broad-reaching regulations, such as Gramm-Leach-Bliley (GLBA) and SOX, many types of businesses must focus on how they safeguard, disseminate, store, and track financial information. Many states have enacted regulations that supersede these federal regulations, however, so ensure that you comply with the pertinent laws in your state in addition to applicable federal regulations.

---

**Note:** The regulations named in this document are specific to the United States of America. Many other countries have similar legislation. Ensure that you understand the regulations where your business operates.

---

Numerous regulations affect how, where, and how long organizations must maintain electronic records, including e-mail. Complying with relevant regulations is complex and should be overseen by legal counsel. The following regulations are pertinent to many organizations and present a good overview of the overall regulatory environment today; however, rely on your legal counsel for applicability to your business.

### Sarbanes-Oxley Act

SOX requires that:

- Executives of publicly traded companies certify the validity of the company's financial statements.
- Financial control and risk mitigation processes be documented and verified by independent auditors.
- Companies implement extensive policies, procedures, and tools to prevent fraudulent activities.

### SEC Rule 17A-4

SEC Rule 17A-4 requires that:

- Original copies of all communications, such as interoffice memoranda, be preserved for no less than three years, the first two in an easily accessible location.
- Records that must be maintained and preserved be available to be produced or reproduced using either micrographic media (such as microfilm or microfiche) or electronic storage media (any digital storage medium or system).

### Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (Financial Institution Privacy Protection Act of 2001, Financial Institution Privacy Protection Act of 2003) was amended in 2003 to enhance protection of nonpublic personal information.

It requires that financial records be properly secured, safeguarded, and eventually completely destroyed so that the information cannot be further accessed.

### Healthcare Insurance Portability and Accountability Act of 1996

HIPAA requires that:

- Security standards be adopted that do the following:
  - Control who may access health information.
  - Provide audit trails for computerized record systems.
  - Meet the needs and capabilities of small and rural healthcare providers.
- Health data be isolated and inaccessible to unauthorized access.
- Transmission of health information is physically, electronically, and administratively safeguarded to ensure confidentiality.

### **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)**

The Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) does the following:

- Requires that financial institutions implement reasonable procedures to maintain information used to verify the identity of a person opening an account with any financial institution.
- Provides law enforcement organizations broad investigatory rights.

### **Department of Defense Rule 5015.2-STD**

Department of Defense Rule 5015.2-STD requires systematic record management, including how records are classified, created, deleted, maintained, reproduced, and used.

### **National Archives and Records Administration**

The National Archives and Records Administration does the following:

- Oversees official government recordkeeping.
- Requires adequate and proper documentation on how U.S. government business is conducted, including the policies and procedures of government agencies.
- Defines records as machine-readable materials made or received by an agency of the U.S. government under federal law or in connection with the transaction of public business.
- Requires that electronic records on a particular subject or function be organized within a record series that facilitates the management of these records.

### **CFR Title 47, Part 42—Telecommunications**

CFR Title 47, Part 42—Telecommunications requires telecommunications carriers to keep original records or reproductions of original records, including memoranda, documents, papers, and correspondence that the carrier prepared or that were prepared on behalf of the carrier.

### **CFR Title 21, Part 11—Pharmaceuticals**

CFR Title 21, Part 11—Pharmaceuticals requires that:

- Controls are in place to protect content stored on both open and closed systems to ensure the authenticity and integrity of electronic records.
- The ability to generate accurate and complete electronic copies of records so that the Food and Drug Administration may inspect them.

---

## Retaining Messaging Data

While many regulations require a specific retention period for business-specific data, not all businesses fall under these requirements; financial services organizations typically have the most stringent data retention requirements. Businesses that are not subject to specific data retention requirements should document their particular data retention policies and, most importantly, *follow* these policies. During investigations, some organizations with clearly defined data retention policies that they nonetheless had not followed have been required to spend innumerable hours restoring and retrieving data from backup media.

Your data retention plans should mesh well with your actual data management processes; for example, if your plan states that e-mail is kept for a year, your backup tapes should not be retained for more than that length of time. Centralized data storage for e-mail and other types of documents (such as a SharePoint Server document repository) ensures that you can easily recover such data in the event that you are required to recover it by legal discovery processes. The ability to preview such documentation, should it be necessary, is helpful when preparing for any legal proceeding.

A number of factors within an organization determine the need for a regulatory compliance solution. Understanding what these factors are and consequently whether an organization needs to implement such a solution typically requires cooperation among a number of groups within the organization. In addition, in driving the organization towards implementing document lifecycle management tools, understanding the needs and requirements of individual groups helps build support for the initiative across the organization.

The three primary components of a regulatory compliance solution for messaging are data archiving, data retention, and data discovery. These components compliment one another, and all organizations that need to meet regulatory compliance rules should consider each of these components before implementing a solution.

### Data Archiving and Retention

It's important to maintain business-critical data in a logical, retrievable manner. The challenge of message archiving is determining:

- What data you need to keep.
- How long you need to keep it.
- Who should have access to the data (or a subset of the data).
- Where you should store the data.

### What Data?

Archive data that pertains to legal, financial, and business decisions according to your organization's data retention policy. E-mail messages relating to lunch dates, personal conversations, and the minutiae of running a business—such as an e-mail message to an administrative assistant regarding the purchase of office supplies—probably does not need to be maintained.

Accurate data archiving with an audit trail is necessary to ensure that all business data is accurately captured and can be verified as original data or as an accurate reproduction thereof. The right data must be captured and stored, and it must be retrievable.

In this solution blueprint, the data archived is primarily messaging data. When envelope message journaling (which is the most inclusive kind of message journaling in Exchange Server) is enabled, all messages from, to, and within your Exchange Server organization are sent to a central journaling

mailbox. The data sent to the journaling mailbox is then queued for delivery to the Enterprise Vault server.

### **How Long?**

Businesses that are bound by the SEC should retain data for no less than seven years. During the first two years of retention, the data must be easily accessible. Other types of industries may have specific regulations regarding their recordkeeping. Be sure that you understand these regulations and their requirements. Companies whose industries are not bound by specific legislation or rulings should define a specific data retention period and enact technical measures to comply with this decision.

As discussed earlier, data retention policies must be in place before beginning any compliance efforts. All stakeholders within your organization must be involved in creating this policy. In particular, IT should not create a policy without input from other departments.

### **Who Can Access the Data?**

Specific trusted individuals may need access to stored data to track communications and to ensure that end users comply with regulations. Access to data should be controlled and audited so that this function is not abused.

Using KVS Discovery Accelerator, an administrator can assign roles to users to control data access and retrieval. These roles let an administrator control which users may access data and how data is reviewed. Authorized reviewers can, for example, quickly target and mark specific data to support legal discovery, compliance-related audits, or investigations.

### **Who Should Manage the Data?**

Ideally, within the organization, corporate librarians manage messaging data archives, just as they manage other important business records; however, few businesses employ corporate librarians to manage their company's data. Even when a company has corporate librarians, they are often underfunded, under-recognized, and under-supported. Yet organizations without corporate librarians still need this function. For companies that don't currently have this role staffed, managing messaging records may be a critical unaddressed need that Microsoft and KVS can help tackle.

Whether a company has a corporate librarian, has a knowledge management team, or lacks a comprehensive strategy, Microsoft and KVS tools can address the need. Businesses that do have corporate librarians or a knowledge management team and strategy can benefit by implementing Enterprise Vault. They gain a single point of management for data that originates from many sources. Because documents from numerous sources (such as Exchange Server databases, file servers, and SharePoint Portal Server sites) are merged into a single Enterprise Vault system, the Enterprise Vault becomes the authoritative information repository.

Corporate librarians and knowledge management teams can use this data repository not only for discovery purposes but also to better understand the business value of the data through analysis and evaluation. For this reason, the knowledge management team should consist of people who understand the vital business nature of the company's data.

Discovery Accelerator provides features for specific data management and retrieval workers. Workers in these roles include:

- **System administrator:** This role creates new cases (a case is a single discovery process), configuring the marking scheme so that messages can be accurately labeled once discovered and creating user roles.

- **Case administrator:** This person manages a case, assigns items to reviewers, and can configure new marking schemes.
- **Reviewer:** Reviewers delve into the data and mark it for further action if necessary.

### Where Should the Data Be Stored?

A centralized data repository makes any discovery processes more efficient and reliable than widely disparate storage systems are. Centralized archiving is the least expensive way to house an archive because it provides the best economy of scale for the storage hardware. Although organizations can use either centralized or distributed archiving, most use a centralized architecture for Enterprise Vault because its caching provides reliable access to the data over long distances and variable electronic link speeds.

Keep all business-related data on servers, and retain messaging data either on the Exchange server or within an archiving system, as detailed later in this solution blueprint. Your end users should never store messaging data in Personal Folders (.pst), because .pst files are not centrally controlled and present an unreliable long-term archival problem.

---

**Note:** Using .pst files on network shares is not supported. For more information, see Microsoft Knowledge Base article “Why Outlook .pst files are unsupported over a LAN or WAN link,” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;297019>.

---

The solution described in this paper uses network attached storage (NAS) running on Windows Storage Server 2003 to host the Enterprise Vault data archive. Windows Storage Server 2003 was chosen because it is simple to deploy, uses familiar technology, and is controllable using a Web interface. It also enables organizations to quickly add storage to their network without the need for intense training. Storage Server can host several terabytes of data and provides dependable storage for your organization's data.

### Data Retention Benefits

Many organizations that implement the solution presented in this paper do so primarily to meet their regulatory compliance needs; however, this solution offers additional benefits beyond regulatory compliance, including:

- Archived data provides a searchable corporate knowledge base. Data can be readily searched for and retrieved by using KVS Discovery Accelerator.
- Global data marking within Discovery Accelerator ensures that data that has already been through a discovery process does not need to be rediscovered and re-reviewed and marked. This reduction in effort is particularly helpful when the scopes of multiple discoveries overlap.
- Records of communications and processes that were previously stored in individual mailboxes can be made available to individuals or groups that were not involved in the initial communication or document approval path. This enables new workers to understand the history behind past business decisions.
- Archived data improves business continuity. The documentation and communications that are essential to the long-term success of your business are available in a single repository that can easily be searched and from which data can be quickly retrieved.
- Archived data increases productivity for users. Because of mailbox size limits, users often have to store e-mail messages in .pst files, leading to the need to search multiple sources for an important

message or document. Enterprise Vault eliminates the need for .pst files and enables users to quickly retrieve data using simple searches when the client tools are installed on each workstation or the Web retrieval tool is available to information workers.

- The ability to verify communications mitigates risk, and document lifecycle management enables businesses to oversee data intelligently.



---

## Message Journaling Considerations

### Standard Message Journaling

Message journaling creates and saves a copy of all e-mail messages received from and sent from, to, and within an Exchange Server information store. Journaling can be enabled globally within an information store or only for specific mailboxes within the information store. (Details on configuration steps to enable message journaling are provided later in this solution blueprint.)

After message journaling is enabled, all messages sent within that information store and sent to and from mailboxes residing on that information store (or for the mailboxes specified) are retained in a specified mailbox. Large organizations, or organizations that send and receive large amounts of e-mail, should dedicate significant resources to the server that hosts the receiving mailbox.

Access to the repository chosen for the message journaling should be carefully controlled. The mailbox is used for the repository. It should also be hidden from the Global Address Book, and permissions to the mailbox should be carefully controlled.

### Exchange Server Envelope Journaling Capabilities

Standard message-only journaling simply delivers a copy of a message flagged for archiving to a designated journal mailbox. For a more complete archive, Service Pack 1 (SP1) for Exchange Server 2003 introduced the Envelope Journaling tool (exejcfg.exe). Envelope journaling delivers archival messages using an envelope message containing a journal report, with the original message as an attachment.

An envelope journal report for an e-mail message contains much more useful information than message-only journaling. E-mail messages comprise numerous attributes. The message envelope, known commonly as P1 data, includes recipient information that was used to route and deliver the message. This recipient information comprises the message headers, including the message originator's e-mail address, one or more recipient e-mail addresses, and, optionally, the protocol extension material. The message contents, known as P2 data, include the body of the message and any other content to be delivered to the recipient, such as the subject line of the message.

---

**Note:** The recipient data that is visible within e-mail clients is defined in the P2 portion of the message. Blind carbon copy (BCC) data is contained in the P2 data of a message and is not visible to the message recipient. For more information about P1 data, see RFC 2821, at (<http://www.ietf.org/rfc/rfc2821.txt>). For more information about P2 data, see RFC 2922, at (<http://www.ietf.org/rfc/rfc2922.txt>).

---

A message journal report includes the transport envelope data associated with the archived message. This envelope data captures all recipient information, including:

- All recipients of the message from the RCPT TO portion of the Simple Mail Transfer Protocol (SMTP) transaction
- The sender identification from the MAIL FROM portion of the SMTP transaction
- Expanded distribution list membership
- Recipients from transport forwarding rules
- The date and time the message was sent and received
- Protocol extension material

Envelope journaling ensures the documentation of all message recipients on the BCC line, recipients from transport forwarding rules, and recipients included in a distribution list—all of which are not reliably documented when standard message journaling is used.

---

**Note:** Microsoft Knowledge Base article “XADM: Bcc Information Is Lost for Journaled Messages in Exchange 2000 Server,” at <http://support.microsoft.com/default.aspx?kbid=810999>, explains how to obtain the hotfix to enable envelope journaling in Exchange 2000 Server.

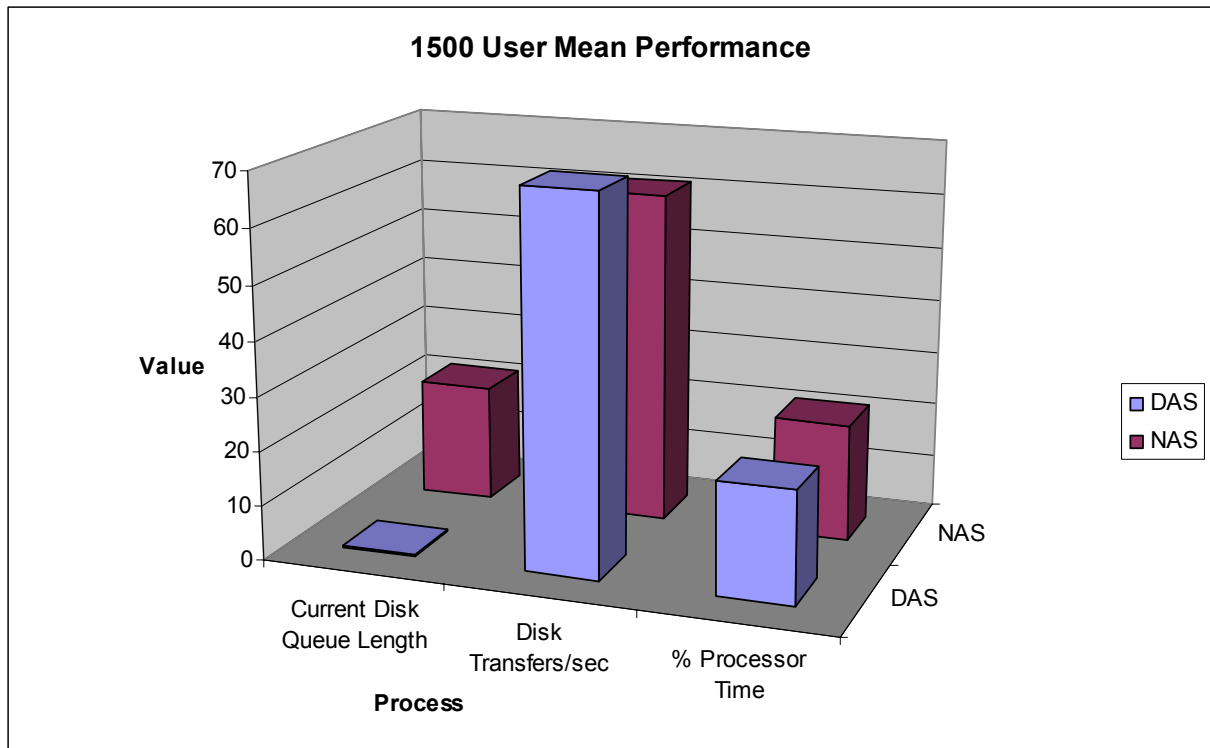
---

Message journaling is enabled on a per-information store basis. Once this functionality is enabled, all messages sent within that information store and to and from mailboxes residing on that information store are retained in either a mailbox or a Public Folder that you specify.

## Message Journaling and Performance

Before enabling message journaling on an Exchange server, consider the performance impact of this operation. Message journaling increases the load on an Exchange server, and careful planning will let you continue to meet current service levels after enabling message journaling. For a simplified, approximate estimate for large organizations, multiply your original resources by 3 to maintain your Exchange servers at their current usage level. Smaller organizations will see less impact on their environments but also must plan to make additional resources available to ensure that service levels do not drop.

The solution that this document presents is for small to medium enterprises (SME), with typically fewer than 3,000 users. A network attached storage (NAS) device built on Windows Storage Server 2003 is hosts the KVS Enterprise Vault archive. Windows Storage Server 2003 provides a flexible, solid foundation for file sharing and storage and is proven a stable, highly responsive platform for Enterprise Vault's archive. Response times within a close range were recorded between NAS on Windows Storage Server 2003 and Direct Attached Storage (DAS) when performance testing simulated 1,500 Exchange Server mailboxes being journaled to Enterprise Vault. The sole difference between the storage solutions was the placement of the drives, which were swapped between a DAS array and the Windows Storage Server array. The Exchange Server 2003 MAPI Messaging Benchmark (MMB3) (<http://www.microsoft.com/exchange/evaluation/performance/mmb3.asp>) was used with LoadSim to gather the performance data. Performance results for the 1,500-user testing are shown in Figure 1.



**Figure 1: 1,500-user mean performance**

### Exchange Server 2003 Message Journaling Planning

Organizations with heavy messaging loads that intend to implement message journaling should plan to install an additional Exchange server to host the journaling mailbox to support:

- A storage group with a single information store that hosts the target mailbox for message journaling.
- Almost two times the normal hardware-related resources, such as disk I/O, RAM, and CPU cycles
- One journal mailbox server (not intended to support MAPI traffic, such as that generated by Outlook clients) for every two to three mailbox servers.
- Sufficient disk space for the information store dedicated to message journaling.

The journaling mailbox on the information store will receive duplicate copies of all e-mail messages sent and received on all journaling-enabled information stores in your organization. (The data within the journaling mailbox is transitory because it is deleted from the journaling mailbox when it is moved into the Enterprise Vault.) Each message is saved in both its original format (.msg) and either HTML or text so that it can be viewed by using the Web browser.

- A dedicated RAID 0+1 (RAID 10, mirroring and striping) volume to host the information store for the best performance.
- Sufficient disk space for the transaction logs.

When messages are journaled, transaction logs are created and can quickly accrue in high-volume situations such as message journaling. Expect high levels of transaction logs because each message that transits the journaling mailbox is also deleted from the mailbox when it is moved into the Enterprise

Vault. The transaction logs will be roughly double in size of what would be expected if all data were simply retained in the mailbox.

- A dedicated RAID 1 (mirroring) volume configured to host the transaction logs for optimal performance.

To ensure that sufficient resources are available, testing within your organization is necessary to determine the exact amount of resources that will be needed to smoothly add message journaling to your environment. Include the following statistics when you gather baseline performance data in your environment to determine your needs:

- The average number of recipients per message. If most messages are sent to large distribution lists in your environment, your resource needs may drop.
- The level of MAPI access to information stores. The performance counters available under the MExchangeIS Mailbox and MExchangeIS Public objects can be logged and analyzed.
- The number of messages handled (sent, received, and submitted) per minute on your current Exchange Server mailbox server.
- The resources in use on your current Exchange server, including the processor (% Processor Time), logical disk (Disk Transfers/sec, Current Disk Queue Length), and memory (Available Mbytes).

Enabling envelope journaling requires additional resources on Global Catalog servers because envelope journaling records the expanded membership of distribution groups. While envelope journaling raises resource requirements, overall the benefits of enabling it outweigh any perceived performance concerns. Without enabling envelope journaling, you might not capture all necessary data, and complying with regulatory compliance is questionable. If your organization heavily uses large universal distribution groups, you may need to add an additional Global Catalog server to your network or dedicate a single Global Catalog server to handle distribution list expansion. (You designate an expansion server by using the Exchange Server Advanced tab on each distribution group's properties page.)

---

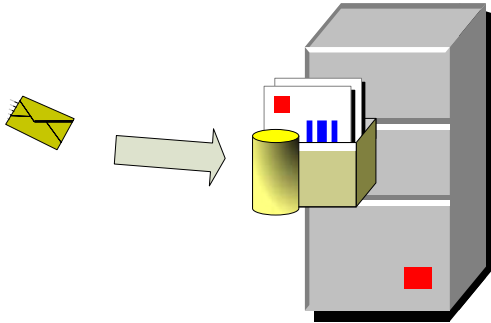
**Note:** Exchange Server 2003 relies on the DSAccess process to determine which Domain Controller and which Global Catalog Server will be used when you need to retrieve directory information. If you want to statically assign a Global Catalog server to provide directory services to Exchange Server, you may do so by following the instructions in the Microsoft Knowledge Base article "Directory Service Server Detection and DSAccess Usage, at <http://support.microsoft.com/default.aspx?scid=kb;en-us:250570&sd=tech>.

---

## Analyzing Data

After you gather performance data from your Exchange server, analyze the data to ensure that adequate resources are available once you enable envelope journaling. This example assumes that without envelope journaling, your mailbox server deals with *X* messages per minute with *Y*% of the resources (CPU, disk I/O bandwidth) used. The goal is to enable envelope journaling and maintain the same resource usage on each server.

Before you enable journaling, each mailbox is dealing with *X* inbound messages per minute with load *Y*%, graphically represented in Figure 2.



**Figure 2: Standard Exchange Server 2003 message traffic**

After envelope journaling is enabled:

- Each mailbox server deals with twice as many messages per minute because the messages are bifurcated.
- You generally need between 1.5 and 2 mailbox servers for each original mailbox server because of the additional load of envelope journaling. This may require deploying an additional Exchange server in your environment if your current server is low on available system resources. (If the total load on all mailbox servers is low, such as 10 percent to 30 percent of resources in use, adding a single journaling mailbox server may be sufficient.)
- You must deploy a dedicated journaling mailbox server to support each two to three mailbox servers.

Figure 3 shows the impact of enabling envelope journaling on Exchange Server and the additional actions performed within the information stores when envelope journaling is enabled.



**Figure 3: Exchange Server 2003 message traffic with Envelope Journaling**

## KVS Enterprise Vault Integration and Features

When KVS Enterprise Vault is deployed, the journaling mailbox sends messages to the Enterprise Vault for long-term archival. The journaling mailbox is used for data in transit between Exchange Server mailbox servers and the Enterprise Vault. Messages in the journal mailbox are deleted as they are moved into the Enterprise Vault. Because Enterprise Vault serves as the long-term repository for all archives, the hardware that hosts the vault data should be sufficiently robust to support this use.

Storage Server provides a solid platform on which to store the Enterprise Vault archive, and through performance testing it has proven capable of handling high levels of usage. It is included in this solution blueprint as the recommended platform on which to host the archive.

Enterprise Vault stores archived messages as individual compressed files. All items are indexed, compressed, and de-duplicated as they are stored. The structure and location of this archive can change as the archive ages, which allows Enterprise Vault to integrate well with information lifecycle management scenarios. De-duplication of messages occurs when the **Share Archived Copies**<sup>1</sup> option is selected on the Enterprise Vault partition. An Enterprise Vault partition is created to host the archived messages and Microsoft SQL Server™ 2000 is used to host the associated configuration and metadata, which enables retrieval of items in the vault. Enterprise Vault's Open Storage Layer allows archived information to be stored using the technology most appropriate for the age of the item. Single items can be concatenated into more efficient collections, and these collections can be automatically migrated to other storage systems—all invisibly to the end user. The Open Storage Layer also gives organizations the flexibility to adopt new storage technologies as they are introduced, thereby protecting the archive over time.

The Enterprise Vault server uses Microsoft published APIs (for the most part, MAPI) to integrate with Exchange Server. The Outlook client can be extended to include an add-on that communicates directly with the Enterprise Vault server (or with its own offline cache if the Outlook client is in Cached Mode)<sup>2</sup>. Extensions are added to the servers hosting Outlook Web Access to ensure seamless access to the messages in the vault.

---

**Note:** The solution presented in this document does not require implementing Enterprise Vault client extensions. The messages must be managed with the KVS Discovery or Compliance Accelerator add-ons to meet regulatory requirements.

---

The configuration and metadata of Enterprise Vault are stored on SQL Server, which provides a solid foundation for retrieval of data within the Enterprise Vault archive. AltaVista Search manages the indexing of the contents of Enterprise Vault. The storage location and optimal size of the index are configurable. To control the size of the index files, Enterprise Vault allows for brief, medium, or full indexing. Brief indexing allows for simple keyword searches. Full indexing allows for more complex searches (at a cost of approximately 12 percent of the archive's size). Archives can be re-indexed at any time to change the index level search, but Microsoft recommends that brief indexing be configured initially.

## KVS Enterprise Vault Discovery Accelerator Integration and Features

KVS Enterprise Vault Discovery Accelerator is a flexible, customizable Web-based tool that enables organizations to efficiently automate the search and discovery of data within Enterprise Vault. To ensure cost-effective, accurate findings when you need to locate data, you can manage content archived in Enterprise Vault by using Discovery Accelerator. Access to the data in Enterprise Vault is customizable and should be limited to designated reviewers. With Enterprise Vault and Discovery Accelerator, there is no need for support from your company's IT team: The need to restore numerous

---

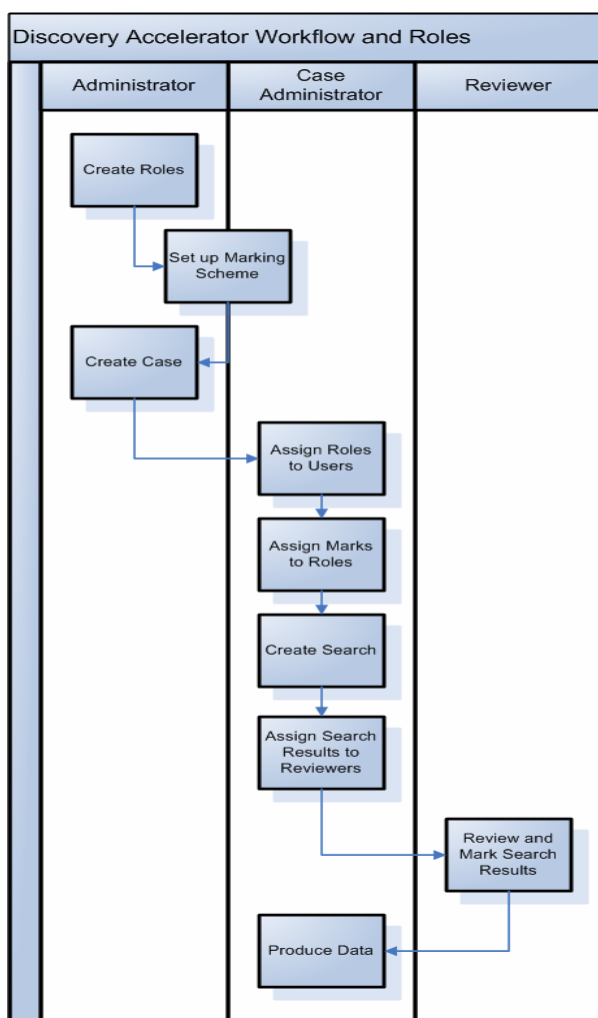
<sup>1</sup> A single instance of each message is stored when multiple recipients have received a message through distribution list, carbon copy, or blind-carbon copy.

<sup>2</sup> Enterprise Vault also has a light client feature that requires only Exchange Organizational Forms. Send an e-mail to [sales@kvsinc.com](mailto:sales@kvsinc.com) or see [www.kvsinc.com](http://www.kvsinc.com) for more information.

backup tapes to disk is gone. The data archive in Enterprise Vault is easily accessible to authorized users without IT interaction.

Discovery Accelerator enables the tracking, marking, and review of data in the Enterprise Vault for litigation support, legal discovery, and investigation. Content within the Enterprise Vault is easily tracked and reviewed and can be marked for further action by authorized reviewers within your organization. Global marking schemes within Discovery Accelerator help organizations avoid duplicating review efforts and make discovery processes more efficient.

A data discovery request means that you need to be able to quickly find, review and organize, and present the data to the appropriate party. Discovery Accelerator smoothes this process and provides controls so that the data is used appropriately. Figure 4 displays the interaction of roles in Discovery Accelerator and shows the process flow of discovery along with the attendant roles and responsibilities.



**Figure 4: Discovery Accelerator workflow and roles**

---

## Implementing the Solution

The solution described in this paper is designed to enable organizations with 3,000 or fewer users to quickly implement a solid platform for their document lifecycle needs and to meet regulatory compliance requirements. Microsoft and KVS together provide solid solutions for data archiving and share the goal of enabling businesses to implement this solution with minimal planning.

Microsoft laboratory testing confirms that the solution architecture and implementation described herein provides a good fit for the SME environment and that Storage Server serves well as the endpoint for the Enterprise Vault archives. Exchange Server 2003 and SharePoint 2003 are well integrated with KVS Enterprise Vault, and the architectures coexist well without numerous custom configuration steps.

### Solution Component Architecture

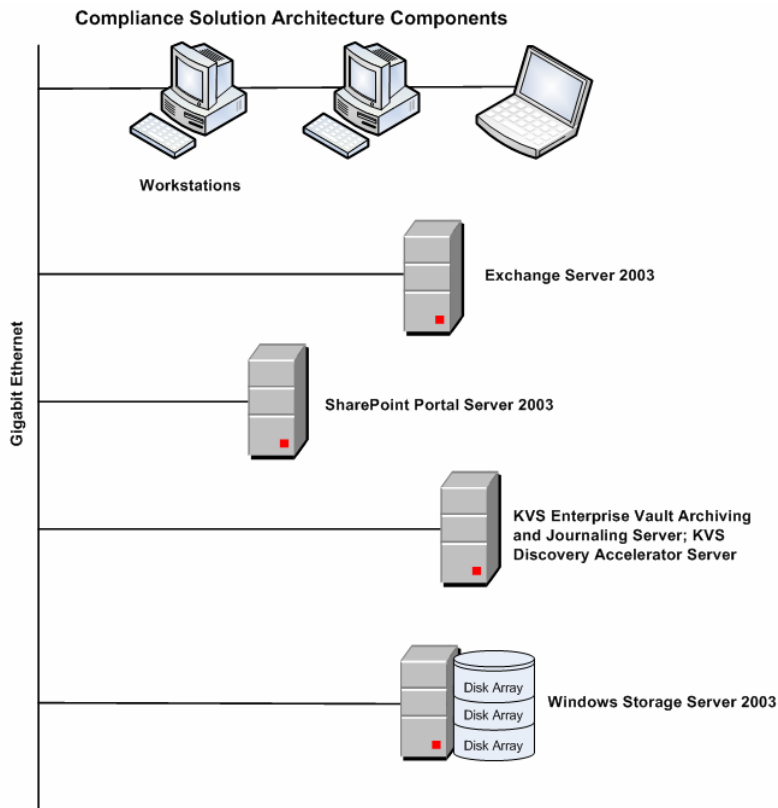
The document lifecycle solution described in this blueprint comprises the following components:

- KVS Discovery Accelerator
- KVS Enterprise Vault
- Exchange Server 2003
- SharePoint Portal Server 2003
- Microsoft SQL Server 2000
- Windows Storage Server 2003

Figure 5 shows the fully implemented solution architecture. How these components fit together in this architecture is discussed in this section.

The solution described in this document assumes that both Exchange Server and SharePoint are deployed in the production environment and that SQL Server is implemented and can support Enterprise Vault. If you have any questions during installation, contact KVS, Inc. at [sales@kvsinc.com](mailto:sales@kvsinc.com) for advice, or visit its Web site at <http://www.kvsinc.com>.





**Figure 5: Solution architecture components**

### KVS Discovery Accelerator

Discovery Accelerator comprises three components:

- **EVDISCOVERY database:** Hosts data such as configuration details, cases that have been created, users and their associated roles, marking scheme templates, searches, and search results.
- **Discovery Service:** Provides control and management for Discovery Accelerator.
- **EVDISCOVERY Web Application:** Provides a management interface to control roles and process flow within Discovery Accelerator.

Discovery Accelerator is installed on Windows Server, usually on the same server that will run Enterprise Vault. You may also install Discovery Accelerator on a separate server than the Enterprise Vault server. If you opt to do so, you must first install Enterprise Vault on the server as described below; you need not perform the configuration steps for Enterprise Vault on a dedicated Discovery Accelerator server.

### KVS Enterprise Vault

Enterprise Vault 5 CP1 must be installed on Windows Server 2003 to support the archive for Exchange Server and SharePoint data. The Enterprise Vault data is stored on a Storage Server NAS device. Every message being sent to, from, or within your organization's Exchange Server environment is journaled into the Enterprise Vault. Generally, Enterprise Vault can compress all items down to 50 percent of their original sizes (some compressed file formats, such as .zip, .jpg, and .gif, cannot be further compressed). Storage requires additional overhead because each item also contains control information of about 5 KB.

### Exchange Server 2003

Exchange is configured to support mailbox journaling. If the current mailbox server is running Exchange Server 2003 Enterprise Edition and has sufficient memory, disk volumes, and processing power to support an additional mailbox store, you may create an additional Storage Group to host a single database that will support the journaling mailbox.

For every 12,500 items journaled per hour in Exchange Server, the load on the Exchange server increases approximately 10 percent. If your current Exchange server is heavily used or is running Exchange Server 2003 Standard Edition, deploy an additional server to host the journaling mailbox.

### SharePoint Portal Server 2003

The data in SharePoint can easily be archived into Enterprise Vault. You do not need to change your current SharePoint configuration. Your current storage point for SharePoint will not change because of this solution; however, any data archived into Enterprise Vault will be stored on Storage Server.

### SQL Server 2000

SQL Server 2000 will support configuration data and metadata for Enterprise Vault, and enables Discovery Accelerator to quickly find and retrieve data. One SQL server is necessary to support four Enterprise Vault servers of equivalent size. The SQL server supporting Enterprise Vault requires a minimum of 1 GB of memory; if additional Enterprise Vault servers are added, additional memory may be necessary. If you will be using a currently deployed SQL server to support Enterprise Vault, ensure adequate system resources are available to support Enterprise Vault. Note that SQL Server is designed to claim all available memory so that the memory is available should the services need it.

SQL server needs approximately 250 bytes of disk space per journaled item. An additional 3 GB of space should be available for static and temporary tables. Regular online maintenance of the SQL database can reduce the size of the entries associated with the journaled items to 169 bytes.

### Windows Storage Server 2003

Windows Storage Server 2003 hosts the data being managed by Enterprise Vault. Data storage needs for Enterprise Vault may be determined by using the following formula:

$$((\text{Number of items}) * (\text{Average item size}) * 0.5) / (\text{Average single instance storage ratio}) + (\text{Number of items}) / (\text{Average single instance storage ratio}) * 7 + (\text{Number of items}) * 2$$

For example, suppose you have 500 items, with an average item size of 10 KB and an average single instance storage ratio of 2.2. The data storage needs would be:

$$((500) * (10 \text{ KB}) * 0.5) / (2.2) + ((500) / (2.2)) * 7 + (500) * 2 = 3727.28 \text{ KB}$$

Single instance storage on Exchange servers is very similar to the de-duplication of messages within Enterprise Vault, and your current single instance storage ratio is a good indicator of how messages will be shared within Enterprise Vault. Single instance storage ratio can be determined by using performance monitor, selecting an information store as the performance object, and selecting single instance storage ratio from the counter list.

Determining the average number of items that are sent and received by your organization, and the average size of these items, is trickier; one way to determine this is by careful analysis of message tracking logs; another way is to enable message journaling for a few days to gather baseline information about how much data is being collected.

**Note:** Windows Storage Server 2003 may not be used to host the Enterprise Vault application because this is contrary to Microsoft's licensing terms. Only the data itself for the Enterprise Vault may reside on Windows Storage Server 2003.

## Creating Your Own Solution

### Introduction

This implementation, which uses Windows Storage Server 2003 Network Attached Storage (NAS), is configured to easily support the integration of KVS Enterprise Vault and Discovery Accelerator into an existing network architecture containing Microsoft Windows Server 2003, Exchange Server 2003, SharePoint Portal Server 2003 (optional), and SQL Server 2000.

Before installing, ensure that you have the KVS 5.0 software, KVS CP1, and a license key from KVS.

### Installation Summary

This solution blueprint guides you through installation to help you meet regulatory requirements. The installation process should follow the steps below. If the steps are not followed in the correct order, the solution may not perform correctly. The configuration process includes:

- Configuring Windows Server 2003
- Configuring Windows Server 2003 Domain Controller, creating a service account in Active Directory to support Enterprise Vault services and access

---

**Note:** This process assumes that the Domain Naming Service (DNS) is integrated with Active Directory and that servers are automatically updating their records in DNS correctly.

---

- Configuring Exchange Server 2003
- Configuring Windows Storage Server 2003
- Configuring SQL Server 2000

---

**Note:** Install the SQL client tools on the Enterprise Vault server or servers and on any server or workstation that will run the Enterprise Vault Administration Console.

---

- Installing and configuring the Enterprise Vault application
- Installing and configuring the Discovery Accelerator

### Configuring Windows Server 2003 for Enterprise Vault, Part 1

Enterprise Vault must run on Windows Server 2003. Configure Windows Server to use NTFS for the file system during installation. Ensure that Internet Explorer, installed on Windows Server 2003 computers by default, is working correctly before you install Enterprise Vault.

You must install the Windows Server 2003 Message Queuing service, the ASP.NET service, and the NNTP component of Internet Information Services (IIS). Have the Windows Server 2003 installation disc available during configuration. When you install these components, be sure you are logged onto the domain with administrator rights.

#### To install the Message Queuing service and the ASP.NET service

1. Click **Start**, and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.

3. In the **Add or Remove Programs** dialog box, click **Add/Remove Windows Components**.
4. In the Windows Components Wizard, select **Application Server**, and click **Details**.
5. Click the **Message Queuing** and **ASP.NET** check boxes.
6. Click **OK**, click **Next**, and then click **Finish**.

#### **To install the IIS components**

1. Click **Start**, and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. In the **Add or Remove Programs** dialog box, click **Add/Remove Windows Components**.
4. Select **Application Server**, and then click **Details**.
5. Select **Internet Information Services (IIS)**, and then click **Details**.
6. Select the **NNTP Service** check box

You may need the original Windows Server 2003 installation CD to install the NNTP service.

7. Select **World Wide Web Service**, and then click **Details**.
8. Select the **Active Server Pages** subcomponents check box.
9. Click **OK** three times.
10. Click **Next**, and then click **Finish**.

You must install Outlook on the Enterprise Vault server and connect it to a mailbox on the Exchange computer before installing Enterprise Vault.

#### **To install Outlook 2003 on the Enterprise Vault Server**

1. Insert a CD-ROM with the Outlook installation code into the Windows Server computer.  
Outlook is on the Office 2003 and Exchange Server installation discs.
2. Browse to Setup.exe on the installation medium you are using.
3. To begin installation, double-click **setup.exe**.
4. Type the product key for the medium, and then click **Next**.
5. Type the **User name**, **Initials**, and **Organization**, and click **Next**.
6. If you agree with the licensing agreement terms, select the **I accept the terms in the License Agreement** check box.
7. Click **Next**, click **Custom Install**, and then click **Next**.
8. Choose to install Outlook and have it run from your computer.
9. Expand the Microsoft Office Outlook object, and click **Collaboration Data Objects**
10. Click **Run from My Computer**, and then click **Install**.
11. After the setup files install, select the **Check the Web for updates and additional downloads** check box.

You may leave the **Delete installation files** check box clear.

12. Click **Finish**, and install any critical or recommended updates.

## Configuring Windows Server 2003 Domain Controller

---

**Note:** You must have a domain controller or a server with the Windows Server 2003 administrative tools installed to configure the domain controller.

---

### To create an Enterprise Vault service account in Active Directory

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the left pane of the **Active Directory Users and Computers** dialog box, double-click the icon displaying your domain name.
3. Right-click **Users**, point to **New**, and click **User**.
4. Type **Enterprise** in the **First name** box; **Vault** in the **Last name** box; and **enterprisevault** in the **User logon name** box.
5. Click **Next**.
6. Type a password that conforms to your security policies, and then confirm it.  
The Vault Service account password cannot be blank.
7. Select the **Password never expires** check box, and click **Next**.
8. Ensure that the **Create an Exchange mailbox** check box is selected.
9. Click **Next**, and then click **Finish**.

---

**Note:** The mailbox you create will be the service mailbox for Enterprise Vault. Archiving, journaling, public folder, and retrieval services will use this mailbox. Do not use it for any other purpose.

---

10. In the left pane of the **Active Directory Users and Computers** dialog box, double-click **Users**.
11. In the right pane of the **Active Directory Users and Computers** dialog box, right-click the Enterprise Vault user object that you created, and click **Properties**.
12. In the **Properties** dialog box, click the **Member Of** tab.
13. Click **Add**, and then type **Administrators** in the **Enter the object name to select** box.
14. Click **Check Names**, and then click **OK** after the name resolves.

### To create an alias in DNS for Enterprise Vault

1. Click **Start**, and point to **All Programs**.
2. Point to **Administrative Tools**, and click **DNS**.
3. Expand your forward lookup zones.
4. Right-click the name of the domain hosting your Enterprise Vault server, and click **New Alias (CNAME)**.

5. In the **Alias name** box, type an alias for the Enterprise Vault directory (such as **entvaultdir**).
6. In the **Fully qualified domain name (FQDN) for target host** box, type the fully qualified name of the Enterprise Vault server.
7. Leave all check boxes in the configuration clear.

### Configuring Exchange Server, Part 1

You must make minor configuration changes to existing Exchange Server 2003 servers to enable message journaling. If the server is running Exchange Server Enterprise Edition, and it has sufficient resource availability, you can enable an additional Storage Group to host the journaling mailbox. If the Standard Edition of Exchange Server is deployed or if the current server is using most of the available hardware resources, you should set up an additional server to host the journaling mailbox. You need an account on the Exchange server with proper permissions, such as Exchange administrator or Exchange full administrator, to complete these steps.

---

**Note:** Be sure SP1 or higher is installed on the Exchange server before proceeding.

---

#### To assign the Enterprise Vault service account permissions in Exchange Server

1. Click **Start**, and then point to **All Programs**.
2. Point to **Microsoft Exchange**, and then click **System Manager**.
3. In the left pane, right-click the Exchange Server organization name, and click **Properties**.
4. On the **General** tab, under **Administrative Views**, select the **Display Administrative Groups** check box if it is not already checked. Click **OK**.
5. Expand **Administrative Groups**, and then expand **First Administrative Group** (or the appropriate administrative group for your organization).
6. Right-click **First Administrative Group**, and click **Delegate Control**. Click **Next**.

---

**Note:** If your organization will use one Enterprise Vault service account for multiple Exchange servers, to delegate control at the organizational level, right-click the organization icon instead of the administrative group.

---

7. To add the Enterprise Vault service account created in Active Directory, click **Add**, and then click the **Browse** button. Click **OK**.
8. Click **Exchange Full Administrator** in the **Role** list.
9. Click **OK**, click **Next**, and then click **Finish**.
10. Click **OK** if prompted.

If necessary, add the Enterprise Vault service account as a local administrator on all Exchange computers.

#### To assign the Enterprise Vault service account permissions to access mailboxes

---

**Note:** Perform these steps on each Exchange server on which Enterprise Vault will be used.

---

1. Click **Start**, point to **All Programs**, point to **Microsoft Exchange**, and click **System Manager**.

2. In the left pane, double-click **Administrative Groups**, and then double-click **First Administrative Group**.
3. To expand the object, double-click **Servers**.
4. Right-click your Exchange server name, and click **Properties**.
5. In the **Properties** dialog box, click the **Security** tab.
6. Under **Group or user names**, click the **Enterprise Vault** service account, and then click **Advanced**.
7. On the **Permissions** tab of the **Advanced Security Settings for Exchange Server** dialog box, click **Add**.
8. Click your **Enterprise Vault** service account from the domain user list, and click **OK** twice.
9. In the **Allow** column of the **Permission Entry** dialog box, select the **Receive As** and **Send As** check boxes. Click **OK**.
10. Click **Apply**, and then click **OK** twice.

### Configuring Windows Storage Server 2003

To support journaling of all messages sent to, from, and within your Exchange Server organization, the Enterprise Vault configuration needs space on the Windows Storage Server. Because data is deleted from the Enterprise Vault according to rules you configure, plan sufficient disk space for messaging data volume in your organization.

OEMs deliver Windows Storage Server 2003 with the base operating system preinstalled and the disks preconfigured. Only simple modifications are necessary.

---

**Note:** Follow the installation instructions that come with your Windows Storage Server NAS devices. The following steps may or may not overlap with the OEM installation instructions.

---

#### To add Windows Storage Server to the domain

1. Click **Start**, right-click **My Computer**, and click **Properties**.
2. Click the **Computer Name** tab, and type a new name that meets your organization's naming conventions in the **Computer description** text box.
3. To add the computer to your Windows domain, click the **Change** button.
4. Confirm this change, and close the **Properties** dialog box.

You need to have permissions within the domain to perform this operation.

#### To configure disks to host Enterprise Vault

1. Click **Start**, and point to **All Programs**
2. Point to **Administrative Tools**, and click **Computer Management**.
3. In the left pane, double-click **Storage**, and click **Disk Management**.

4. Ensure that the disks you want to use for the Enterprise Vault storage are formatted with the NTFS file system and are in an appropriate RAID 5 configuration for the data. Assign a drive letter to the disks.
5. Click **Start**, and then click **Windows Explorer**.
6. Right-click the disk volume that you formatted, and click **Sharing and Security**.
7. Click **Share this folder**.
8. Name the shared folder appropriately, and note the name for future use.

---

**Note:** Microsoft recommends using a hidden shared folder.

---

9. Click **Permissions**, and then click **Add**.
10. Type the name of the Enterprise Vault service account in the **Enter the names to select** box, and then click **Check Names**.  
  
If necessary, click the Enterprise Vault service account name in the list.
11. Click **OK**—twice if necessary.
12. Highlight the service account name, and select the **Full Control** check box.
13. Click **Apply**, and then click **OK** twice.

To create the Vault Store partition, you must first create a folder on the disk volume on which it will reside.

#### **To create a folder in the disk volume for Enterprise Vault**

1. Click **Start**, and then click **Windows Explorer**.
2. Expand the disk volume you created for Enterprise Vault.
3. Right-click the empty right pane, point to **New**, and then click **Folder**.
4. In the text box, type **Message Journal**.

#### **Configuring Windows Server 2003 for Enterprise Vault, Part 2**

##### **To add the Enterprise Vault Service account to local administrators**

1. Click **Start**, right-click **My Computer**, and click **Manage**.
2. In the left pane, double-click **Local Users and Groups**, and then click **Groups**.
3. In the right pane, double-click **Administrators**.
4. In the **Properties** dialog box, click **Add**.
5. In the **Enter the object names to select** dialog box, type the name of the Enterprise Vault service account that you created earlier.
6. Click **Check Names**, and select the account you created.

After you configure the service account for Enterprise Vault, you need to create an Outlook profile for the Enterprise Vault mailbox.



### To create a profile for the Enterprise Vault mailbox in Outlook

1. Click **Start**, and then point to **All Programs**.
2. Point to **Microsoft Office**, and then click **Microsoft Office Outlook 2003**.
3. In the Outlook setup wizard, click **Next**.
4. In the Account Configuration window, click **Yes**, and then click **Next**.
5. In the E-mail Accounts window, click **Microsoft Exchange Server**, and then click **Next**.
6. Under **Microsoft Exchange Server**, type the name of an Exchange server in your organization.
7. Under **User Name**, type the name of your Enterprise Vault service account.
8. Click **Check Name**, **Next**, and then **Finish**.

The SQL client tools must be installed on the Enterprise Vault server and on any other computer that will be used to administer Enterprise Vault.

### To install the SQL Client Tools

1. Insert the SQL Server 2000 CD into the server's CD-ROM drive.
2. Click **Start**, click **Run**.
3. In the **Run** dialog box, click **Browse**, and find and open \X86\setup\setupsql.exe.
4. To install SQL Server, click **OK**.
5. In the **Welcome** dialog box, click **Next**.
6. In the **Computer Name** dialog box, ensure that **Local Computer** is selected.
7. In the **Installation Section** dialog box, click **Create a new instance of SQL Server, or install Client Tools**, and click **Next**.
8. In the text box, type your name and company information, and click **Next**.
9. Read the software licensing information, and if you agree with the licensing requirements, click **I Agree**.
10. Click **Next**.
11. In the **Installation Definition** dialog box, click **Client Tools Only**, and click **Next**.
12. In the **Select Components** dialog box, select the **Management Tools** and **Client Connectivity** check boxes, and clear the check boxes for **Books Online** and **Development Tools**.
13. Click **Next** after confirming the settings, and then click **Next** again if prompted regarding Microsoft Data Access Components (MDAC) setup.
14. Click **Finish** (if prompted by the MDAC setup).
15. After the SQL tools install, select the **Yes, I want to restart my computer now** check box, and click **Finish**.

Obtain and install the latest Service Pack for SQL Server 2000, available at <http://www.microsoft.com/sql>.

---

**Note:** To work properly on Windows Server 2000, SQL client tools require SQL SP 2 or later. You will need the database components.

---

#### To install the Exchange System Management Tools

1. Insert the Exchange Server CD into the CD-ROM drive.
2. Browse to the **setup\i386** directory.
3. To install the Exchange System Management Tools, double-click **setup.exe**.
4. Close all other programs, and click **Next**.
5. Read the licensing agreement, and click **I agree** if you do.
6. Click **Next**.
7. Next to **Microsoft Exchange** in the Action column, select **Custom**.
8. Next to **Microsoft Exchange System Management Tools** in the Action column, select **Install**, and click **Next**.
9. Be sure that the data in the **System Summary** dialog box is accurate, and click **Next**.
10. After installation completes, click **Finish**.

#### To create a persistent drive mapping to the Shared Windows Storage Server 2003 Disc

1. Click **Start**, and then click **Windows Explorer**.
2. Click **Tools**, and then click **Map Network Drive**.
3. Specify a drive letter that is not in use, and type the path to the Windows Storage Server 2003 drive that you shared earlier.
4. Be sure that the **Reconnect at logon** check box is not selected, and click **Finish**.

#### To install Enterprise Vault

1. Click **Start**, and then point to **All Programs**.
2. Point to **Administrative Tools**, and then click **Services**.
3. Right-click **IIS Admin Service**, and then click **Stop**.
4. To stop the IIS Admin Service and several other services, click **Yes**.
5. Put the Enterprise Vault CD in the CD-ROM drive.
6. Browse to the **Enterprise Vault <version>\Enterprise Vault\Server** directory, double-click **setup.exe**, and click **Next**.
7. Read the licensing agreement; click **Yes** if you accept it.

---

**Note:** To ensure that the software will install in the correct directory, leave the default setting **C:\Program Files\Enterprise Vault**.

---

8. Click **Next**, and be sure that the **Enterprise Vault** and **Administration Console** check boxes are selected.
9. Click **Next**, and confirm that the program folders to be used are appropriate for your environment. Click **Next** again.
10. In the installation dialog box, click **Next**, and confirm your settings.
11. In the **Installation Complete** dialog box, ensure that the **Run the Configuration** check box is selected, and click **Finish**.
12. To ensure that a new Vault directory installs on this server, in the Enterprise Vault Configuration Wizard, be sure that **Yes** is selected, and click **Next**.
13. Type the name of the Enterprise Vault service account you created earlier, and type the service account password twice to confirm it. Click **Next**.
14. To confirm that the service account you designated has been granted permissions to log on as a service, act as part of the operating system, and debug programs, click **OK**.
15. In the **SQL Server location** text box, type the name of your computer running SQL Server 2000, and click **Next**.

---

If you want to create the database in a named instance of SQL Server 2000, instead enter the instance in the format **<server name\instance name>**.

---

16. Enter the locations where you want to store the database and the transaction log files.
17. To create the Enterprise Vault directory, click **Next**.
18. Type a name and description for the Vault Site.
19. Type an alias for DNS to use for the Vault Site.

This can be the name of the Enterprise Vault server and should be fully qualified.
20. Click **Next**, and confirm that the next DNS alias will correctly identify the Enterprise Vault computer.
21. Click **Next**, and type the password for the Enterprise Vault service account. Click **Next** again.
22. Read the information regarding the services, click **Next**, and click **Add**.
23. Select **Enterprise Vault Retrieval Service**, and add the name of the Exchange server that will host the journaling mailbox in the Exchange Server area. Click **Next** again.
24. Confirm the locations of the services, and ensure that the **Run archiving service in report mode** check box is selected. Click **Next**.
25. Click **Use this mailbox**, and click **Browse**.
26. Click the Enterprise Vault service account mailbox in the list, and click **OK** twice.
27. To start the Enterprise Vault services, click **Next**.
28. To confirm that you want to start the services, click **Next** again.
29. To close the configuration program, click **Finish**.

Ensure that your Enterprise Vault license key is named Keys\_computername.txt and in place in the **Program Files\Enterprise Vault** directory.

#### To create an Enterprise Vault Store

1. Click **Start**, and then point to **All Programs**.
2. Point to **Enterprise Vault**, and then click **Administration Console**.
3. In the **Directory Service Computer** text box, type the name of the Enterprise Vault server, and click **OK**.
4. In the **Enterprise Vault Administration Console**, double-click **Enterprise Vault**.
5. Click **Directory** on <server name>, and then select your Enterprise Vault store alias.
6. Right-click your Vault Store, point to **New**, and then click **Vault Store**.
7. Click **Next** twice.
8. Type a name and description for the new Vault Store, and then click **Next**.
9. Type the name (or named instance) of the computer on which you want to store the Vault Store database.
10. Enter appropriate locations for the Vault Store database and log files on this computer, and click **Next**.  
  
Leave the default settings in place for safety copies and automatic creation of Vaults.
11. Click **Next**, and then click **Finish**.
12. To add a Vault Store Partition to the new Vault Store, click **Next**.
13. To create the partition, click **Next**.
14. Name the partition, and type a description for it.

---

**Note:** Alternatively, you can accept the suggested name and description.

---

15. Ensure that **Open** is selected, and click **Next**.
16. Click **Network Share**, and click **Next**.
17. Type the name of the network share and the folder you created in Windows Storage Server 2003 in the format \\servername\sharename\$**Message Journal**.  
  
Be sure to include the \$ (dollar sign) if you created a hidden share.
18. Click **Next**, and select the **Share archived items** and **Create Vault Store Partition with security ACLs** check boxes.
19. Click **Next**, and click **None** in the list.
20. Click **Next** again, and click **Finish**.

#### To create a Vault

1. Click **Start**, and then point to **All Programs**.
2. Point to **Enterprise Vault**, and then click **Administration Console**.

3. Type the name of the Enterprise Vault server to identify the **Directory Server**.
4. Double-click **Enterprise Vault**, double-click **Directory on Enterprise Vault**, and then double-click the name you chose for the server's Directory alias.
5. Right-click **Archives**, point to **New**, click **Vault**, and then click **Next**.
6. Click the Vault Store you created above, and then click **Next**.
7. Type a name and description for the new Vault, and then click **Next**.
8. Click **Add**, and add the Enterprise Vault service account to the **Add Names** area.
9. In the **Type of Access** list, click **Control**, and then click **OK**.

---

**Note:** If you want others to have access to this Vault, you can either select those names now or add them later.

---

10. Review your choices, and then click **Next**.
11. Leave the indexing service options at their defaults, and then click **Next**.
12. Leave the **Use site setting** check box selected.
13. To add a billing account, click the **Browse** button, and select a user account from your domain.
14. Click **OK**, click **Next**, click **Finish**, and then click **Close**.

#### To add the Enterprise Vault Journaling Service

1. Click **Start**, and then point to **All Programs**.
2. Point to **Enterprise Vault**, and then click **Administration Console**.
3. Type the name of the Enterprise Vault server.
4. Double-click **Enterprise Vault**, double-click **Directory on Enterprise Vault**, and then double-click the name you chose for the server's Directory alias.
5. Double-click **Computers**.
6. Right-click the Enterprise Vault server icon, point to **New**, and then click **Service**.
7. Click the **Enterprise Vault Journaling Service**, and add the name of the Exchange server that will host the journaling mailbox in Exchange Server.
8. Click **Add**.
9. To configure the Journaling Service, click **Yes**.
10. To select the mailbox to use as your journaling destination, click **Browse**, click the mailbox in the list, and then click **OK**.
11. To select the Vault to use for journaling, click **Browse**, click **Apply**, and click **OK**.
12. Type the password for the Enterprise Vault service account, and click **OK**.

#### To start Enterprise Vault services

1. Click **Start**, point to **Administrative Tools**, and click **Services**.

2. Scroll to the Enterprise Vault services listings in the Services MMC.
3. To change the setting of any Enterprise Vault service from **Disabled** or **Manual** to **Automatic**, right-click the service, click **Properties**, change the **Startup Type** to **Automatic**, and click **OK**.
4. If any Enterprise Vault service's status is Stopped, right-click the service and click **Start**.

## Configuring Exchange Server, Part 2

### To enable Message Journaling

1. Click **Start**, and then point to **All Programs**.
2. Point to **Microsoft Exchange**, and then click **System Manager**.
3. Double-click **Administrative Groups**, and browse to the Administrative Group hosting your Exchange server.
4. Double-click **First Administrative Group** or the administrative group that hosts your Exchange server.
5. Double-click **Servers**, and click the Exchange server on which you want to enable journaling.
6. Expand the appropriate Storage Group (usually **First Storage Group**).
7. Right-click **Mailbox Store**, and then click **Properties**.
8. On the **General** tab of the **Mailbox Store Properties** dialog box, select the **Archive all messages sent or received by mailboxes on this store** check box.
9. Click **Browse**, and either type the journaling mailbox name in the **Enter the object name to select** text box or use the **Advanced** option to find the name in the address list.
10. Click **OK**, click **Apply**, and then click **OK**.

## Configuring SQL Server 2000

### To create an SQL logon for the Enterprise Vault Service Account using SQL Enterprise Manager

1. Click **Start**, and then point to **All Programs**.
2. Point to **Microsoft SQL Server**, and then click **Enterprise Manager**.
3. In the left pane, double-click **SQL Server Group**, and then double-click **local**.
4. In the right pane, double-click the **Security** folder.
5. Right-click **Logins**, and on the shortcut menu, click **New Login**.
6. In the **Name** text box, type the name of the Enterprise Vault service account in the format of **domain name\service account**.
7. Ensure that **Windows Authentication** and the correct domain name for the account are selected.
8. Under **Security Access**, ensure that **Grant access** is selected.
9. On the **Server Roles** tab, select the **Database Creators** check box, and click **OK**.

## Configuring Windows 2003 Server for Discovery Accelerator

Discovery Accelerator installs on the Windows 2003 server that runs Enterprise Vault.

Discovery Accelerator needs the Internet Explorer WebControls to install and run correctly. WebControls are available in the Redistributables folder on the Discovery Accelerator CD.

### To install the Internet Explorer WebControls

1. Insert the Discovery Accelerator CD into the CD-ROM drive of the Enterprise Vault server.
2. Browse to the **Redistributables** folder.
3. Double-click **IEWebControls.exe**. If prompted, click **Open**.
4. Read the terms of the licensing agreement, select **I accept the terms in the license agreement** if you agree with the terms, and click **Next**.
5. Leave the installation path in its default configuration, click **Next**, and click **Finish**.

### To set temp folder access for the IIS Worker Process User

1. Right-click **Start**, and click **Explore**.
2. Click **My Computer**, and then click **Local Disk (C:)**.
3. Right-click **temp** (if there is no **temp** folder, create one), and click **Properties**.
4. Click the **Security** tab, and click **Add**.
5. Type **Network Service** in the **Enter the object names to select** text box.
6. Click **Check Names**, and click **OK**.
7. Ensure that **Network Service** is selected, and in the **Allow** column, click **Full Control**.
8. Click **Apply**, and then click **OK**.

### To install the Discovery Accelerator Software

1. Log on to the Enterprise Vault server using the Enterprise Vault Service Account you created earlier.
2. Insert the Enterprise Vault installation CD into the CD-ROM drive of the server.
3. Right-click **Start**, and click **Explore**.
4. To open the Enterprise Vault installation CD, in Windows Explorer, browse to the server's CD-ROM drive, and double-click it.
5. To open Enterprise Vault 5.0 CP1 directory **\\Discovery Accelerator\\Kit**, double-click it, and then double-click **setup.exe**.
6. On the **Welcome** screen, click **Next**.
7. Read the licensing agreement, and click **Yes** if you agree with it.
8. Type a **User Name** and **Company Name** in the area provided.
9. Ensure that **Anyone who uses this computer** is selected, and click **Next**.
10. Select **Typical**, and click **Next**.

11. Review the settings, click **Next** if they are correct, and click **OK**.
12. Type the Enterprise Vault Service Account name in the format of **domain\username**.
13. Enter and confirm the password in the correct fields.
14. Click **OK**, and click **Finish**.

#### To install the license key for Discovery Accelerator

1. To get a license key, send the C:\Program Files\KVS\Discovery Accelerator\EVSystemInfo\_Computername.txt file to KVS .

---

**Note:** <Computername> should be the NetBIOS name of the Enterprise Vault server.

---

2. Copy the Keys\_computername.txt file that KVS returned to you, and paste it into the **C:\Program Files\KVS\Discovery Accelerator** directory.
3. Click **Start**, point to **Administrative Tools**, and then click **Services**.
4. Right-click **Enterprise Vault Discovery Accelerator Service**, and then click **Start**.
5. Close the Services applet.

#### To configure Discovery Accelerator

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery** in the address bar.
4. On the **Discovery Accelerator** home page, click **Configure**.
5. In the **SQL Server** text box, type the name of the SQL Server 2000 computer or instance that supports Discovery Accelerator.
6. In the **Database name** box, leave **EVAccelerator** in place.
7. In the **Data file folder** text box, type the drive that will host the database file.

---

Drive locations should be valid, existing paths on the SQL Server computer and may be local or mapped drives.

---

8. In the **Log file folder** text box, type the drive location that will host the database file.
9. In the **Directory DNS Alias** text box, type the DNS alias or server name of the Enterprise Vault Directory Service computer, and click **OK**.
10. Click **Start**, point to **Administrative Programs**, and then click **Services**.
11. In the **Services** applet, right-click **Enterprise Vault Discovery Accelerator Service**, and then click **Restart**.
12. Close the **Services** applet.
13. Change to the **Discovery Accelerator** home page, and click **OK**.



---

## Discovery Accelerator in Action

The EVDiscovery Web Application is the main interface for Discovery Accelerator. You use it when you need to find data within Enterprise Vault. The main uses of the EVDiscovery Web Application are:

- Creating cases
- Assigning an administrator to a case
- Creating users
- Creating and assigning roles for users
- Setting up marking schemes such as "personal," "spam," or "relevant"
- Creating searches, after which another search with defined parameters is created
- Assigning reviewers for data returned in a search
- Allowing reviewers to use defined marking schemes to annotate items returned in a search
- Exporting reviewed items so that they can be presented

When a governing body receives a request for information, the company should create a knowledge-management team. A knowledge management team usually comprises representatives from the legal department and corporate librarians. The IT department does not need to be actively involved in this process.

To designate the responsibilities of each team member, roles should be explicitly assigned, as Figure 4 shows. You can customize permissions when you assign roles; however, assign as few permissions as possible. The permissions you assign might vary, depending upon the size of your organization and the size of the team assigned to the discovery process.

---

**Note:** The EVDiscovery Web Application interface reveals only the tasks for which user who is currently logged on has permissions to complete.

---

The following instructions walk you through the EVDiscovery Web Application, creating a case, searching for data, marking the data, and the production of the data. This process follows the workflow shown in Figure 4. For this discovery exercise, imagine that the following team is responsible for discovery in your organization:

- **Senior legal department representative:** The system administrator who oversees all cases
- **Legal department representative:** The case administrator who manages the case day-to-day
- **Corporate librarians:** The reviewers who mark the search results

Although the IT department does not have an active role in managing cases, IT must help set up the first case and administer the system.

The IT representative initially creates roles to be assigned to the other team members.

### To create roles in Discovery Accelerator

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.

3. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
4. In the **Application Administration** column, click **Roles**, and then click **New Role**.
5. In the **Name** text box, type **Case Administrator**.
6. In the **Description** text box, type a description, such as **Team Leader**.
7. For **Scope**, select **Case**.
8. Under **Permissions**, select the **Case Administration**, **Search**, **Assign**, **Production**, and **Review** check boxes, and click **OK**.
9. Click **New Role**. In the **Name** text box, type **Reviewer**.
10. In the **Description** text box, type a description, such as **Corporate Librarian**.
11. Under **Permissions**, select the **Review** check box, and click **OK**.

Scheme templates exist globally in Discovery Accelerator and serve as templates for marking schemes created in cases. Do not change any scheme templates at first, but check to ensure that the default Review Marks scheme template—which serves as the base scheme for all marking—exists. If you ever intend to create a new scheme template, you will use this interface.

#### To review scheme templates

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
4. In the **Application Administration** column, click **Scheme Templates**.
5. Ensure that the **Review Marks** template, with a description of **Review Marks**, exists.

Marks are used when reviewing search results. The default marks and their definitions are as follows:

- **No mark:** The item has yet to be reviewed.
- **Relevant:** The item is relevant to the current discovery.
- **Not relevant:** The item is irrelevant to the current discovery.
- **Query:** The item has yet to be queried for the search.

Every mark is assigned a status. For example, the status of a relevant item would be **Included**, while the status of a mark of not relevant would be **Excluded**.

In the following procedure, you name a new mark so that you can easily classify unsolicited commercial e-mail (UCE) messages. When this mark is applied to an item returned in queries, the item will retain the marking and the messages can be excluded from examination during other case reviews.

#### To create marks in Discovery Accelerator

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
4. Click **Marks** in the **Application Administration** column, and click **New Mark**.

5. Type **UCE** in the **Name** text box.
6. Type **Unsolicited Commercial E-mail** in the **Description** text box.
7. Click **Reviewed** in the **Status applied** list.
8. Select the **Items retain this mark for use in other cases** check box, and click **OK**.

After you create a new mark, you must add it to the scheme template so that WHO can use it when marking items searched in a case. The following steps add the UCE mark to the existing scheme template.

#### To add a mark to a scheme template

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
4. In the **Application Administration** column, click **Scheme Templates**, and then click **Review Marks**.
5. In the **Edit Template** dialog box, click **Next**.
6. Select **UCE** and click the right angle bracket (>), and click **Finish**.

WHO uses Discovery Accelerator cases to oversee data discovery. When discovering data, WHO must create a case to manage the process and isolate the results of the search for review, marking, and production. Use the Discovery Accelerator Web interface to perform this operation. In the following procedure, you create a case for widget trading and assign case ownership to your team legal representative.

#### To create a case in Discovery Accelerator

1. Log on to the server using the Enterprise Vault Service Account.
2. Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
3. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
4. In the **Application Administration** column, click **Cases**, and then click **New Case**.
5. In the **Name** text box, type a name for the case, such as **Widget Trading**.
6. Next to the **Case Owner** box, click **Add User**.
7. In the **Add User** dialog box, type the case administrator's user name in the format **domain\user name**. The case owner is also called the "administrator."
8. Click **Close**.
9. In the **Vault Stores** box, select the vault store (or multiple vault stores) to include in the case.
10. Leave the **Next export number** and **Size of the export ID** boxes set to their default values.
11. In the **Prefix** text box, type a prefix relevant for the search results  
This prefix should clearly relate to the case name; in this case, **Widget** is appropriate.
12. In the **Output folder** text box, type the path where the results should be written, such as **C:\caseoutput\case name**, and click **OK**.

The administrator assigns roles to other users. After the administrator assigns the case administrator role, that person can also assign roles to other users.

#### To assign roles to users

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Type the case administrator's password and user name in the format **domain\username** if prompted.
4. In the **Case Administration** column, click **Widget Training** (the case name).
5. Under **Options**, click **User Roles**, and click **Add User**.
6. In the **Login** name box, type the name of the team member whom you want to add in the format **domain\username**, and click **Add**.
7. Repeat steps 8 and 9 to add all the team members, and click **Close**.
8. In the **Roles** column, click **Admin**.
9. In the **Users** column, select the check box for each user who needs administrator rights for the case.
10. In the **Roles** column, select **Case Administrator**.
11. In the **Users** column, select the check box for each user who needs to have Case Administrator rights for the case.
12. In the **Roles** column, select **Reviewer**.
13. In the **Users** column, select the check box for each user who needs reviewer rights for the case, and click **OK**.

You use marks when reviewing items returned from a search. You can restrict specific users to using only permitted marks for search items; however, in the following procedure, all reviewers may use all marks. Administrator rights are necessary to perform this operation.

#### To assign marks to roles

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Type the administrator's password and user name in the format **domain\username**.
4. In the **Case Administration** column, click **Widget Training** (the case name).
5. Under **Options**, click **Schemes**, and then click **Review marks**.
6. In the **Edit Scheme** dialog box, click **Next**.
7. In the **Scheme Marks In Review Marks** dialog box, click **Next**.
8. Click **Reviewer**, and then select the check boxes for all the marks.
9. To assign marks to other roles, select the role, select the check box for each mark the role should be able to assign to an item, and then click **Finish**.

Targets are users for whom you can search in cases. Target groups are groups of users for whom you can search. To include all data in a search, you do not need to create targets. To create target groups, you need administrator's or case administrator's rights. In the following procedure, you create a target for one user and then add that user to a target group.

#### To create targets

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Enter the case administrator's password and user name in the format **domain\username** if prompted.
4. In the **Case Administration** column, click **Widget Trading** or the appropriate case name.
5. Under Options, click **Address Manager**.
6. Click **New Target**.
7. In the **First Name** text box, type the user's first name.
8. In the **Last Name** text box, type the user's last name.
9. In the **Email Addresses** text box, type **address@domain.com**, click **OK**, and then click **Close**.
10. Click **New Group**.
11. In the **Name** text box, type a name for the group, such as **Test Group**.
12. In the **Description** text box, type a description, such as **Testing**.
13. Click **Edit Targets**, and select the check box for the target added earlier, and click **OK**.

Discovery Accelerator lets you search for specific information within vaults. Case administrators and other roles with search permission may create searches. Carefully control who may create searches, and clearly document what keywords searches have used. You do not need to complete the search options fields if you want to search a wide range. You can perform multiple searches, using different keywords, in a single case.

#### To search Enterprise Vault

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Enter the case administrator's password and user name in the format of **domain\username** if prompted.
4. In the **Case Administration** column, click **Widget Trading** or the appropriate case name.
5. Under **Options**, click **Searches**, and then click **New Search**.
6. In the **Search name** text box, type a name for the search, such as **Widget**.
7. Click the calendar icon next to the **Date from** box, and select the starting date for the search.
8. Click the calendar icon next to the **To** box, and select the last date to include in the search.
9. Choose from the following search options, and then click **OK**:

- To isolate the message's originator or to select multiple originators, select the address book icon. Then select the appropriate check box for the target users or groups, and click **OK**.
- To isolate the message's recipient or to select multiple recipients, double-click the address book icon. Then select the appropriate check box for the target users or groups, and click **OK**.
- To search for a specific word or phrase in the subject line of messages that your search returned, type the word or phrase (such as **widget**) in the **Subject** text box.
- To isolate a word or phrase in the message body or in a message attachment, type the word or phrase (such as **widget trades**) in the **Content** text box.

10. To view a result, click it.

11. Click **Accept**, and then click **Close**.

12. In the **Search Accepted** dialog box, click **Close**.

Assign the items that your search returns to designated reviewers for marking.

#### To assign search results to reviewers

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Enter the case administrator's password and user name in the format of **domain\username** if prompted.
4. In the **Case Administration** column, click **Widget Trading** or the appropriate case name.
5. Under **Options**, click **Review Assignment**.
6. In the **Role** list, click **Reviewer** or the role assigned to your reviewers.
7. To assign each reviewer a number of items from your search, in the **Assign** column in the **Name** list, type a number.
8. Click **Apply**, and then click **Close**.

Reviewers mark their search items as appropriate for their pertinence to the matter at hand; if items are not necessary for production, they should be marked as excluded from the case. Items that need to be produced should be marked as included. Each designated reviewer will follow the steps presented within this section. When reviewing search results, reviewers can filter messages within the case, or begin at the first message within their case.

#### To review and mark search results

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Enter the reviewer's password user name and in the format **domain\username** if prompted.
4. In the **Reviewer** column, click **Widget Trading** or the appropriate case name.

The items you assign to current users appear under **Your Items**, in the **Case Status** row. The number of items your search returns is listed under **All Items**.

5. The following options help you filter messages assigned to a reviewer:
  - **Items:** Enables the reviewer to view only those items assigned to him or her.
  - **Mark:** Lets the reviewer view their items by their current mark, such as **Relevant**, **Not Relevant**, or **No Mark**.
  - **Status:** Enables the reviewer to view their items by their status, such as **Included**, **Excluded**, or **Pending**.
  - **Search:** Enables the reviewer to view their items by a particular search or from all searches.
  - **Go to:** Option lets the reviewer select which item to view.
6. Leave all options under **Options** in their default states, and click **OK**.
7. To review the text of the first item to be reviewed, move the scroll bar.
8. Type any comments in the **Comment** box.

Others can see and use comments for further review.
9. Use the **Mark** option to select a mark for the item, such as **Relevant**, and click **Next**.
10. Repeat steps 9 and 10 for each item.
11. After you review all the items, either close the browser or click **Home** to go to the Discovery Accelerator home page.

After all the items from a case are marked, you might have to send them to external governing bodies, such as the SEC, for review. The following procedure produces all items marked **Included** from the sample case above.

#### To produce items

1. From any computer, click **Start**, point to **All Programs**, and then click **Internet Explorer**.
2. To open the Discovery Accelerator home page, type **http://<servername>/evdiscovery**.
3. Enter the case administrator's password and user name in the format **domain\username** if prompted.
4. In the **Case Administration** column, click **Widget Trading** or the appropriate case name.
5. Under **Options**, click **Production**, and then click **Select Items**.
6. Select **Included** in the **Status** box.
7. In the **Number of items** box, enter the number of items to produce.

---

Note: If many items are available, you might want to produce only a portion of the items at first.

---

8. Click **OK**, click **Close**, and click **New Run**.
9. In the **Name** text box, type a name for the production run.
10. In the **Number of items** box, type the number of items to produce.
11. Click **OK**, and then click **Close**.

12. After the run completes, click **Start**, click **Run**, and then type **C:\caseoutput\case name**, as you designated when you created the case. Then click **OK**.

13. Double-click the name you used for the production run in Step 11.

The items that were produced should be within this folder; you may now copy the items to other media that can be provided to external governing bodies.



---

## Installing and Configuring Optional Solution Components

After you install and configure KVS Enterprise Vault and Discovery Accelerator, you might want to enabling SharePoint Portal Server 2003 archiving.

### Enabling SharePoint Portal Server 2003 Archiving

If you want, you can archive data from SharePoint sites in a separate Vault Store . Doing so provides a repository of project-related documents, enabling your organization to easily retrieve data that is no longer active. You can continue to use SharePoint for projects are in process. Keep the Vault Store you use for SharePoint data separate from the Vault Store that hosts journaled data from Exchange Server.

**Note:** To allow backward compatibility, the Enterprise Vault SPS Service installs only if SharePointclient components are installed on the Enterprise Vault server. You can download SharePoint client components from the SharePoint CD or from <http://www.microsoft.com/downloads/details.aspx?FamilyID=DF39E250-F7AE-445A-AC9D-A80C9035ED6B&displaylang=en>.

---

#### To configure Enterprise Vault to support SharePoint data

1. Log on to the Enterprise Vault server using the Enterprise Vault Service Account.
2. Click **Start**, and then point to **All Programs**
3. Point to **Enterprise Vault**, and then select **Administration Console**.
4. In the **Directory Service** Computer box, type the name of the computer running the Enterprise Vault Directory Service that you want to use, and click **OK**.
5. Double-click **Enterprise Vault**.
6. Double-click **Directory on <server name>**.
7. Double-click **<directory server alias>**.
8. Double-click **Computers**.
9. Right-click the Enterprise Vault computer you want to support SharePoint Portal Server 2003, point to **New**, and select **Service**.
10. Select **Enterprise Vault SPS Service**.
11. Type the name of the SharePoint Portal Server to use in the **SharePoint Portal Server** box and click **Add**.

### Supplemental Installation for End-User Archive Access

#### Adding an Archiving Service for Users

Optionally, you can create a separate Vault Store to let information workers archive their mailbox data. Doing so can help keep infrequently used data accessible but outside the Exchange Server information store. Never archive mailbox data in the Vault Store used for message journaling. Your organization might need data in that store, and data needed for legal purposes should not be mixed with other data.

Use the Enterprise Vault Configuration program to create a new Vault Store, and install the Enterprise Vault Archiving Service on the Enterprise Vault server. Doing so lets information workers archive their data.

### Requirements for Users' Computers

To archive mailbox items, information workers must have user extensions must be installed on their workstations. When user extensions are installed, users can search, view, and restore archived messages from all Outlook client versions. To use these extensions, the workstation must be running one of the following operating systems:

- Windows Server 2003
- Windows 2000
- Windows NT Server Version 4.0 with SP 6a or later
- Windows XP Professional
- Windows 2000 Professional
- Windows NT Workstation Version 4.0 with SP 6a or later
- Windows Millennium Edition
- Windows 98 with DCOM 98 1.3 or later
- Windows 95 OSR2 or later with DCOM for Windows 95

When a message is archived from an information worker's mailbox, the message is moved from the Exchange Server information store into the appropriate Vault store for the Enterprise Vault Archiving Service. A shortcut is created on the Exchange server that links the archived message to the original message data. This shortcut displays the **From** and **Subject** lines of the message. You can customize what users see when they click a shortcut by using the following options:

- **Show contents:** Double-clicking the shortcut displays the item's contents in their original format.
- **Show properties:** Double-clicking the shortcut displays the properties of the shortcut.

Alternatively, you can install Outlook Web Access extensions on the Exchange servers, enabling access to the Enterprise Vault archive. For this task, you need Internet Explorer 5.01 or later.

You can set up mailbox archiving globally and create rules to enable automatic archiving of data in mailboxes. You can grant information workers discretion over archiving their mailbox data. Default retention categories can be used to enable smart data retention, and customized retention categories may be created to provide more flexible data archiving.

When an information worker's mailbox is enabled for message archiving, a welcome message is automatically sent to the mailbox. This message tells information workers how to take advantage of Enterprise Vault features. You can edit these messages to include information on installing the Enterprise Vault user extensions.

---

## Conclusion

Meeting regulatory requirements is an ongoing process. You should comprehend the process well before you implement a long-term message archiving system. To ensure that your organization creates and follows clear policies, you must thoroughly understand its messaging capabilities and needs and the processes and technology.

With this solution blueprint, your company can immediately realize the benefits of a message archiving and retrieval solution that extends the native message journaling capabilities of Exchange Server. Implementing KVS Enterprise Vault and Discovery Accelerator can help your organization meet regulatory requirements.

This document guides you through installing and configuring numerous Windows Server technologies, such as Exchange Server, SharePoint Portal Server 2003, KVS Enterprise Vault, and KVS Discovery Accelerator. The flexible storage solutions of Windows Storage Server 2003 let your organization quickly and easily implement large disk arrays to support the storage needs of Enterprise Vault. Enterprise Vault, in turn, provides an unparalleled collection of tools to help both users and your organization exploit the message archive. Users can view the hierarchy of all archived information in the feature-rich Archive Explorer client, which does not require deployment. By following this solution, your organization can retain its e-mail and documents, model the retention against corporate guidelines, and quickly and easily discover content as needed.

---

## Related Links

See the following resources for further information:

- "Introduction to Windows Storage Server 2003 Architecture and Deployment," at <http://www.microsoft.com/windowsserversystem/wss2003/techinfo/plandeploy/wss2k3archdeploy.mspx>.
- "An update rollup is available to enable the Envelope Journaling feature in Exchange 2000 Server," at <http://support.microsoft.com/?kbid=834634>.
- "Server Consolidation Using Exchange Server 2003," at <http://www.microsoft.com/downloads/details.aspx?FamilyId=BC3A8D76-FC58-4E3C-9152-1CE35E9466EA&displaylang=en>.
- For the latest information about Windows Storage, see the Microsoft Storage Web site, at <http://www.microsoft.com/storage>.
- For the latest information about Windows Server 2003, see the Windows Server 2003 Web site, at <http://www.microsoft.com/windowsserver2003>.
- For the latest information about Exchange Server 2003, see the Exchange Server Web site, at <http://www.microsoft.com/exchange>.
- For the latest information about KVS Enterprise Vault and Discovery Accelerator, see <http://www.kvsinc.com>.